ARMY REGULATIONS
No. 335–5

WAR DEPARTMENT,
WASHINGTON, *July 1937.*

SIGNAL COMMUNICATION AND CRYPTOGRAPHIC SECURITY

SECTION I

GENERAL

1. **Preliminary.**—*a.* No authorized code or cipher will be employed by any person who has not read these regulations.

b. A copy of these regulations will be filed in the container in which code books are filed.

2. **Signal communication security.**—*a.* The secrecy with which signal communication can be conducted contributes materially to the success of military operations. This necessitates establishing and preserving signal communication security, the purpose of which is to nullify enemy efforts to learn the meaning of the messages. Aside from the serious and incalculable military consequences which may follow from violations of regulations established for safeguarding cryptographic material and messages prepared by their means, the financial loss attendant upon the compromise of a code or a cipher system is a serious matter. A code which has cost thousands of dollars and required the services of expert compilers over a period of many months may be rendered worthless by a few poorly encoded messages or by carelessness in handling the translation of a single message.

b. The most important means of attaining signal communication security is the effective use of cryptography.

3. **Cryptographic security and the principal factors upon which it depends.**—*a.* Cryptographic security is that branch of signal communication security which deals with the preparation of technically sound cryptographic systems, their proper usage, and their careful safeguarding.

*This pamphlet supersedes AR 335–5, June 10, 1936.

146466°—37

b. The degree of cryptographic security afforded by a given system is measured by the amount of resistance which messages cryptographed in that system present to enemy cryptanalysis. This depends upon four interdependent factors—

(1) The technical soundness of the system.
(2) The amount of text available for study.
(3) The safeguards placed about the practical employment of the system.
(4) The skill and organization of the enemy cryptanalytic services.

4. **Influence of the amount of text available for study.**—The amount of text available for study greatly influences the speed and ease with which messages can be solved. The amount of text available depends upon a number of factors, among which are the following:

a. The distribution of the system, that is, the number of headquarters permitted to use it.

b. The restrictions placed upon its use at those headquarters, that is, the types of messages which may be cryptographed in the system, the number of persons permitted to employ it, and for what purposes.

c. The agencies of signal communication employed in transmitting the messages, which usually determine whether the traffic is interceptible, and if so, at what ranges.

d. The technical procedure followed in transmission, which often determines whether or not messages will have to be repeated in whole or in part, thus giving further opportunity for interception.

e. The extent and efficiency of the enemy intercept organization.

5. **Influence of the safeguards placed about the practical employment of the system.**—By far the most prolific sources of danger to cryptographic security arise from violations of principles governing the following:

a. The physical security of all technical paraphernalia pertaining to the cryptographic systems.

b. The drafting of messages to be transmitted by signal communication agencies susceptible of enemy interception, and their classification into the three classes, "Secret", "Confidential", and "Restricted", as provided in AR 330–5.

c. The selection of the specific cryptographic system, and the actual cryptographing.

d. The handling and filing of literal, paraphrased, and cryptographic versions of messages.

e. The preparation of information copies and press releases in which information contained in cryptographed messages is communicated to others.

f. The selection of the transmission means and the procedure followed in transmission.

SECTION II

AUTHORIZATION, PREPARATION, AND DISTRIBUTION OF CODES AND CIPHERS

6. **By whom authorized.**—*a.* Cryptographic systems vary widely in technical soundness, depending upon the principles underlying their construction. It is practically impossible to devise a cryptographic system which is impregnable against solution by a well-organized, highly trained group of cryptanalysts.

Sooner or later the messages can be solved and whether solution will be achieved "sooner" rather than "later" depends entirely upon the other factors mentioned above. The preparation of technically sound cryptographic systems for practical usage is a difficult matter and must therefore be entrusted to experts.

b. All codes, ciphers, and cipher devices intended for employment within the Military Establishment will be authorized only by the Secretary of War, except that codes or ciphers for special purposes within field forces may be authorized by the Commanding General, GHQ.

c. The use of any unauthorized code, cipher system, or cipher device for cryptographing official messages is forbidden.

d. The use of any authorized code, cipher system, or cipher device for cryptographing personal messages is forbidden.

7. By whom prepared and distributed.—*a.* Authorized codes, cipher systems, and cipher devices will be prepared and initially distributed only by the Chief Signal Officer.

b. The signal officer of a field or expeditionary force may be directed to take over the responsibility for the preparation and distribution of replacement editions of field codes and of cipher alphabets and keys for use with authorized cipher systems. Until such time, however, the preparation and distribution of field codes and ciphers will continue to be a responsibility of the Chief Signal Officer.

c. Unit signal or communication officers, acting under orders from local commanders, may prepare, revise, and distribute *only for local use* cipher alphabets and keys for authorized cipher systems. They may prepare, revise, and distribute *only for local use* special supplements to authorized codes where and to the extent that provision has been made for such supplements.

SECTION III

PHYSICAL SECURITY, STORAGE, ISSUE, AND TRANSPORTATION

8. Individual responsibility for physical security.—The provisions of AR 330–5, dealing with "Secret", "Confidential", and "Restricted" documents, are basic in connection with individual responsibility for safeguarding cryptographic material. This section is concerned with details of the subject as they apply specifically to cryptographic material. For United States Statutes governing the protection of official documents, see section VI.

9. Regulations governing storage.—*a.* All registered cryptographic material will be kept in the most secure storage space available, which should be at least a three-combination safe. Except as indicated in *b* below, only commissioned officers whose duties require that they use this material will be permitted to handle it and to have access to the containers thereof.

b. At stations within the continental limits of the United States and in the oversea departments, warrant officers, specially selected enlisted men, and United States Civil Service employees may be permitted to have access to the safe or containers of cryptographic material.

c. All codes, ciphers, and material pertaining thereto will be kept in their properly assigned storage whenever they are not actually in use.

d. So far as practicable, cipher tables, alphabets, and keys will be kept in separate containers from the code books, publications, and devices to which they apply.

e. Whenever the custodian leaves the room, safes containing cryptographic material will invariably be locked by the full combination.

f. At each headquarters an inspection will be made daily, immediately before the close of business, to insure that all cryptographic material has been properly stowed away, and that all safes, cabinets, windows, and doors in the room are locked.

10. Issue, custody, and replacements.—*a.* The Chief Signal Officer establishes and maintains the central office of issue for all cryptographic publications, codes, cipher systems, and cipher devices. He may establish or designate intermediate issuing offices for direct distribution to tactical units.

b. Codebooks, cipher systems, devices, alphabets, and keys will be issued only to commanding officers of a headquarters and according to authorized distribution tables or Tables of Basic Allowances.

c. The commanding officer may designate the unit signal or communication officer to act as custodian of the cryptographic material issued to the headquarters, but this will in no way relieve him from his responsibility for this material.

d. When cryptographic material has become unserviceable through long usage, request for replacement will be made to the issuing authority.

11. Regulations governing transportation.—*a. Transmission of documents.*—See AR 330–5.

b. Opening of sealed containers.—Prior to opening a sealed package or envelope containing cryptographic publications or similar documents, a careful inspection of the seals and wrappers of the package will be made to ascertain whether the package has been subjected to any tampering. If any evidences of such tampering are noted, the facts will be immediately reported to the issuing authority in order that an investigation may be made without delay.

SECTION IV

INVENTORY, ACCOUNTING, AND REPORTS OF CRYPTOGRAPHIC MATERIAL

12. Inventory and accounting.—Every custodian of cryptographic material will keep at all times a complete inventory of the material in his custody. Accounting of this material will be made in accordance with the provisions of this section, using the authorized forms.

13. Report of receipt.—Receipt of registered secret or confidential codes, ciphers, cipher devices, and publications relating thereto will be acknowledged immediately by the person to whom issued directly to the Chief Signal Officer,

Washington, D. C., in time of peace, and in the case of the field forces in time of war directly to the signal officer, GHQ.

14. Report of transfer.—*a.* When registered cryptographic items are transferred from one person to another, a certificate of transfer in triplicate will be accomplished. The certificate will be dated and signed by the transferring officer and will contain an acknowledgment of receipt by the receiving officer.

b. Immediately upon completion of the transfer, the original of the certificate of transfer will be forwarded directly in time of peace to the Chief Signal Officer, Washington, D. C., and in the case of the field forces in time of war directly to the signal officer, GHQ. A copy of the certificate of transfer will be retained by each of the transferring and receiving officers.

15. Report of possession.—*a.* Persons in the possession of registered secret or confidential codes, ciphers, cipher devices, and publications pertaining thereto, will render a semiannual report thereof on June 30 and December 31 of each year. This report will be made to the Chief Signal Officer, Washington, D. C., in time of peace, or in the case of the field forces in time of war to the signal officer, GHQ.

b. In making a semiannual report of possession, the following details will be observed:

(1) Each item will be sighted and its register number checked against the inventory. Merely making a copy of the preceding report without actually sighting the item and checking its register number is forbidden.

(2) At headquarters having two or more commissioned officers, the custodian and one other disinterested officer will make the inventory and both will sign the report. At headquarters having only one commissioned officer, the report will state that fact.

c. No semiannual report of possession will be made on training editions of codebooks, cipher alphabets, or keys, nor will such reports be made on cipher devices which do not bear register numbers and which are accounted for as is ordinary property. However, all such items will be safeguarded so as to prevent compromise.

d. Whenever a person to whom registered secret or confidential codes, ciphers, cipher devices, and publications pertaining thereto have been issued has no further need therefor, he will report that fact to the Chief Signal Officer, Washington, D. C., in time of peace, or in the case of field forces in time of war to the signal officer, GHQ.

16. Reports of destruction, compromise, or discovery.—*a.* When a cryptographic document has been declared obsolete and its destruction authorized by competent authority or by instruction in a superseding document, it will be destroyed by burning, unless otherwise directed. In the case of secret items this will be done by or in the presence of a commissioned officer, who will draw up and sign the report certifying to the destruction.

b. If a secret or confidential cryptographic document is lost, or if even a suspicion arises that it has been compromised in any manner whatsoever, the facts will be reported to the issuing authority by fastest secret means possible. The commanding officer of the headquarters to which the lost or compromised publication is charged will conduct a thorough investigation for the purpose of determining all pertinent facts.

c. Whenever a registered cryptographic publication is discovered which is not charged to the finder, it will be forwarded at once to the commanding officer of the headquarters. If the latter's records do not show the proper holder, he will report the matter to the issuing authority, who will direct disposition of the item.

17. Use of short titles.—*a.* In making up a semiannual or transfer report, an ordinary report of destruction, or in any ordinary document or correspondence in which complete titles are not essential, short titles will be employed, and such reports or correspondence need not be classified. See AR 330–5.

b. The use of short titles or of abbreviated designations as indicators in cryptographed messages is forbidden.

SECTION V

REGULATIONS GOVERNING DRAFTING, CLASSIFYING, AND FILING CRYPTOGRAPHIC MESSAGES

18. Drafting messages.—*a.* The plain-text wording of cryptographic messages has a vital bearing upon their security. Standardization in content and form in documents such as field orders, operation instructions, and the like is necessary, but when fixity in expression is carried over into message construction the results are exceedingly dangerous to cryptographic security. Hence, stereotyped phraseology and set form of expression, especially at the beginnings or ends of messages, will be avoided at all times.

b. Words not important to the sense will be omitted. Conjunctions and prepositions will be reduced to a minimum and every effort will be made to avoid repetition of words.

c. The originator of a secret, confidential, or restricted message will paraphrase such portions as are quoted from—

(1) A message in plain language,

(2) A message in the same or another cryptographic system, or

(3) A newspaper, periodical, or public document.

d. Words instead of figures will be used in expressing numbers except in meteorological messages.

e. The frequently unnecessary punctuation words such as "stop", "period", "comma", etc., afford excellent clues to the solution of messages. They will be avoided whenever possible. Following the rules of commercial practice, punctuation marks should be spelled out in all cases when it is essential that they be transmitted in the body of the message.

19. Classifying messages.—*a.* The originator of a message will be responsible for the determination of the need for secrecy and for the classification he gives it, unless special instructions governing particular cases have been received from higher authority.

b. The originator of a message will be responsible that the classification he gives it ("Secret", "Confidential", or "Restricted") conforms to the definitions given in AR 330–5, and that the message is properly marked as to classification before being forwarded for cryptographing and transmission. The tendency to give messages a higher classification than is really warranted by the subject matter will be curbed so that unnecessary employment of secret or confidential codes and ciphers can be avoided.

c. In order to prevent the cryptographing of *identical* subject matter by means of *different* codes and ciphers, once a message has been classified, all subsequent messages on the same subject will normally be similarly classified. A change in classification is dangerous to cryptographic security. For this reason correct initial classification is very important. However, if it becomes advisable or necessary to change the classification because the situation has become more serious than was originally foreseen, the change will be authorized by the senior officer of the group of communicants. *In such cases, references to previous messages by their reference numbers will be avoided.*

d. Routine reports and messages which must be given a wide distribution, or the contents of which may eventually be furnished the press, or which contain extracts or quotations from a newspaper, periodical, or similar public document, are always a source of great danger to cryptographic security. Such reports and messages will be prepared so as to permit their transmission in plain language, or at most they will be classified as "Restricted."

e. A mere acknowledgment of receipt of a cryptographed message will invariably be classified as a plain-language message so that it will not be cryptographed.

20. Selecting the cryptographic system.—*a.* The selection will be governed by the originator's classification, a "Secret", "Confidential", or "Restricted" system being selected to correspond with the originator's classification. However, if the message center chief believes that the message has been incorrectly classified, or that it contains definite violations of the rules governing the drafting of such a message, he will bring the matter to the attention of the officer in charge.

b. When the same message must be sent to two or more addressees (the texts being absolutely identical), they will all be cryptographed absolutely identically. If, however, this is impossible because all the addresses do not possess identical codes or ciphers, then the text of each message which must be cryptographed in a different system will be carefully paraphrased before cryptographing. See paragraph 26.

c. If two or more messages to different addressees present only minor differences in wording so that if cryptographed exactly as written by their originator the cryptograms would be practically identical, paraphrasing will be resorted to in order to destroy cryptographic similarities. See paragraph 26.

d. When, under the conditions set forth in paragraph 19c, later messages are given a higher classification than have been given the early ones on the same subject, a shift to an appropriate cryptographic system will be made.

e. Great care will be taken to insure that a new code, cipher, cipher alphabet, or cipher key is not employed before the effective date and hour.

f. The use of a confidential or secret cryptographic system for cryptographing matter which has appeared in a newspaper, periodical, or other public document is forbidden. Such matter will as a rule be sent in plain language or at most in a restricted system. When such matter is germane to the context of a confidential or secret message, and must be quoted verbatim, the quotation will be made in a separate message in a restricted code or cipher and the confidential or secret message will contain only a statement to the effect that the quotation is being sent separately.

21. **Cryptographing and decryptographing, when, where, and by whom performed.**—*a.* A message will invariably be cryptographed under the following circumstances:

(1) When it contains information which is secret or confidential except that when, in the judgment of the originator, the necessity for getting the information to the addressee without any delay is so urgent that this consideration completely outweighs the value that its interception in plain language would have for an enemy. Such a message will bear the notation "Send in clear" over the signature of the originator.

(2) When it contains matter the transmission of which in plain language is prohibited by AR 105–25.

(3) When a saving in time or cost of transmission can be effected by the use of a code permitting condensation or abbreviation of the text.

b. At all headquarters where message centers are authorized, cryptographing and decryptographing of all messages sent or received in code or cipher will be performed at the message center, under the supervision of the signal or communication officer of the headquarters concerned, except that meteorological messages may be cryptographed and decryptographed by meteorological personnel by means of special codes provided for the purpose.

c. The cryptographing and decryptographing of messages by means of secret or confidential codes or ciphers will be performed only under the direct supervision and as the definite responsibility of a commissioned officer. It is preferable that commissioned officers perform all cryptographing and decryptographing. However, within the discretion of the commanding officer, warrant officers, trusted enlisted personnel, or civilian employees who are American citizens and in whom the commanding officer has implicit confidence, may be authorized by him to cryptograph and decryptograph secret or confidential messages under the supervision of a commissioned officer. Such authorization will be in writing, and no person not so authorized will be permitted to handle or use secret or confidential codes or ciphers.

22. **Mixing of plain and cryptographic text forbidden.**—*a.* Except as indicated below, no plain language whatever will appear in the text of a cryptographed message.

b. The following are the only exceptions to the rule in *a* above:

(1) When no special method of indicating reference numbers and dates is provided as a part of the cryptographic system involved, the sender's serial number of message and the day of the month spelled in letters will be left in plain language at the beginning of the text of a cryptographed message.

(2) If the use of a code or cipher indicator is authorized, the indicator will appear in plain language (uncryptographed) after the serial number of message.

(3) If shown on the message blank, the time of origin of the message will be left uncryptographed.

c. Cryptographers will be especially watchful to see that plain language does not creep into the text of a cryptogram by inadvertence or carelessness in transferring text from worksheets on to message blanks.

23. Addresses and signatures.—*a. Peacetime regulations.*

(1) Where dispatches are sent to offices such as "Commanding Officer, Fort Slocum, N. Y.", or "Quartermaster, Fort Slocum, N. Y.", the addresses used will be as given above rather than as "Lieut. Col. Jones, Infantry, C. O., Fort Slocum, N. Y."

(2) Where a dispatch is sent to a subordinate in an office or command, the dispatch will be addressed to the commanding officer of the office or command. The name of the subordinate will be given in the first part of the body of the message preceded by the word "For." Example: A dispatch for Capt. John Doe, Headquarters, Second Corps Area, will be addressed "Commanding General, Second Corps Area, Governors Island, N. Y." For Capt. John Doe, etc. (in body of dispatch).

(3) Dispatches will be signed with the surname of the sender. Where the surname alone is not sufficient to enable the addressee to establish the official position of the sender it will be followed by such essential additional information as will fix definitely the official capacity of the sender.

b. Wartime regulations.

(1) In the theater of operations, in messages which are transmitted in normal or abbreviated form between field units in tactical nets (radio, wire, telephone, visual), the tactical call signs of the units will serve as addresses and signatures. Neither address nor signature will appear in the text. At the receiving message center the official designation of the addressee and of the sender (as indicated by the call signs appearing in the heading) will be inserted in the positions reserved for these items on the authorized field message blank.

(2) In the zone of the interior special address and signature codes may be issued, in which case they will be used in accordance with instructions accompanying them.

24. Arrangement of cryptographic text.—*a. All code or cipher* messages will be written and transmitted in groups of a maximum of five characters, except as follows:

(1) In meteorological codes, groups of more than five figures are permissible when transmitted by Government radio.

(2) In the case of field or tactical messages, the groupings authorized in the code will be observed.

b. Under no circumstances will the original word lengths be retained in the case of cipher messages, no matter by what agency or means they are transmitted.

25. Repeating messages.—*a.* Repetition of messages in whole or in part is dangerous to cryptographic security and will be reduced to a minimum.

b. Errors introduced by telegraphy can be readily corrected by calling upon the transmission agency for repetition of the incorrect groups. This merely gives more opportunity for enemy interception. But errors introduced by

cryptography are much more dangerous. Their correction will be made only with the approval of the officer in charge of the message center.

c. If an addressee telegraphs the sender that he is unable to decryptograph a message and requests repetition, it is absolutely forbidden to do any of the following:

(1) Transmit the original literal plain text.

(2) Transmit a corrected version of the first cryptogram if the latter had been incorrectly cryptographed, that is, if the procedure to be employed was incorrectly performed even in the slightest detail.

(3) Cryptograph the message in the correct code or cipher if an incorrect one had been used through blunder, and retransmit.

d. If transmission of the contents of the message in the foregoing case is essential and cannot be done by messenger, the entire message will be most carefully paraphrased, cryptographed correctly or in the proper code or cipher, and retransmitted.

26. Paraphrasing.—*a.* To paraphrase a message is to rewrite it so that its meaning is the same but its phraseology is different. It is an essential procedure in the cases cited under paragraphs 20*b* and *c*, and 25, and in the case of messages prepared in any secret or confidential code or cipher, the contents of which must be given a wide distribution or communicated to the press.

b. In paraphrasing it is not sufficient to paraphrase only the beginning or end of the message; the entire message will be subjected to the process. The original text will be condensed rather than expanded.

c. Paraphrasing consists in applying *all* the following processes to the message:

(1) Changing the sequence of the paragraphs.

(2) Changing the sequence of the sentences in each paragraph.

(3) Shifting the positions of the subject, predicate, and modifiers in each sentence.

(4) Changing from active to passive voice or vice versa.

(5) Substituting synonyms or equivalent expressions.

d. When paraphrasing must be resorted to in connection with messages having identically or nearly identically plain texts (see pars. 20 *b* and *c*, and 25), effort will be made to change the lengths of paraphrased versions so that the cryptograms will not resemble each other even in that respect.

e. A paraphrase of a message will be accorded the same classification and will be handled exactly the same as the original message would be handled.

27. Handling and filing messages.—*a. Outgoing secret messages.*

(1) The originator will prepare and number all copies, this being done only under the direct supervision and as the definite responsibility of a commissioned officer. The originator will send the original copy to the message center and will retain one carbon copy for temporary file. Other carbon copies (all numbered) may be circulated, for the information of local officers directly concerned, in which case each information copy will bear the following notation: "The making of an exact copy of this message is forbidden. Only such extracts as are absolutely necessary will be made and marked 'SECRET.' This copy will be safeguarded with greatest care and will be returned to the originator without delay." After their return all information copies will be destroyed by burning.

(2) The original copy sent to the message center will be cryptographed. In the case of message centers serving tactical units, one original and one carbon copy of the cryptographed message will be made, and the original will be sent to the transmitting agency. In the case of message centers serving fixed headquarters in the zone of the interior, the number of copies of the cryptographed message will be determined by the commanding officer of the headquarters concerned. *All* work sheets connected with the cryptographing of the message will be immediately destroyed by burning.

(3) The original copy of the literal plain text will be marked "Sent in secret code" and will be returned to the originator. Upon receipt of the original copy of the literal text, the originator will place it in his special secret file for outgoing secret messages, and will destroy the temporarily retained carbon copy by burning. There will be but one copy of the literal text on file at the originator's office.

(4) The transmitting agency will transmit the cryptographic message and will retain at least one copy thereof in its file of outgoing messages, for final disposition in accordance with local regulations.

b. Incoming secret messages.

(1) The incoming message will be copied in duplicate by the receiving operator. The original will go to the cryptographic section of the message center, the carbon copy to the files of the receiving station, where it will be disposed of in accordance with local regulations.

(2) In the cryptographic section a cryptographer will decryptograph the message and will make one and only one copy of the decryptographed literal (plain) text, which will be marked "Received in secret code", and delivered to the addressee. The cryptographed version will be retained in the files of the message center, where it will be disposed of in accordance with local regulations. All work sheets connected with the decryptographing will be destroyed by burning. The cryptographing section will *not* retain any copy of the plain text in its files. The placing on the message blank of any marks or indications even remotely connected with the cryptographic system or steps in decryptographing the message (such as underlining key words, indicating groupings corresponding to lengths of columns of a key, etc.) is forbidden.

(3) The decryptographed message having reached the addressee, the latter may make and circulate a limited number of carbon copies for the information of other officers directly concerned, in which case they will bear the same notation as indicated under *a* (1) above. After their return all information copies will be destroyed by burning. There will be but one copy of the literal text of the message at the addressee's office.

c. Confidential and restricted messages.—Insofar as practicable the procedure to be followed in the case of messages to be transmitted in confidential and restricted codes or ciphers will be substantially the same as in the case

of messages to be transmitted in secret codes or ciphers, except that the messages will be marked and handled according to the general regulations governing confidential and restricted documents as set forth in AR 330–5.

d. Under no circumstances will a copy of the cryptographed message ever be filed with or attached to a copy of the equivalent plain-text message; nor will work sheets bearing an interlinear translation of a cryptographed message be retained in files at the cryptographic section.

e. At stations having no regularly constituted message centers, the services specified to be performed by personnel at regularly constituted message centers (*a* to *d* above) will be performed either by the originator of the message or by personnel specifically assigned to these duties by the commanding officer of the station. The resulting cryptogram will be forwarded to the telegraph or cable company. The literal text of the message will be retained in the secret files of the originator in a secure safe. He will also retain a copy of the cryptogram, but this will never be filed together with the literal version, or even in the same safe.

28. Confirmation copies.—As a general rule confirmation copies of messages transmitted in code or cipher will *not* be sent by mail or otherwise.

29. Precautions regarding press releases.—*a.* Officers authorized to prepare information to be made public will constantly bear in mind that such material is of great value in enemy signal intelligence work. They will exercise great caution to prevent the release of information which has been received or sent in cryptographed messages and which may be directly correlated with specific messages, such as verbatim quotations or extracts citing names of persons, places, dates, hours of the day; specific details of the results of an action; the number and types of casualties; number of prisoners taken; number and types of matériel captured, etc. The less specific the information disclosed in a press release, the safer from the standpoint of cryptographic security.

b. The regulations governing paraphrasing messages will be strictly observed by all concerned in the preparation of press releases and communiques. See paragraph 26.

30. Destruction of documents to avoid compromise.—*a.* When it has become certain that cryptographic publications and translations of messages will be subject, in wartime, to capture, or in peacetime in the event of a disaster such as fire or earthquake, to theft or compromise, all such material and paraphernalia will be destroyed by burning.

b. Cipher machines and cipher devices will be destroyed beyond use or repair under the same circumstances.

31. Selection of signal communication agency.—*a.* A signal communication agency susceptible of enemy interception will not be employed for transmitting a message when another agency not susceptible to interception and equally effective can be used.

b. In the combat zone, conditions permitting, messages going only a very short distance, or very long messages will ordinarily be sent by messenger. Means of signal communication other than radio, which will be taken into consideration from the point of view of reducing the amount of interceptible traffic, are as follows:

(1) Telephone (except near front lines).
(2) Telegraph (except near front lines).
(3) Buzzerphone.

(4) Messenger.
(5) Visual (when not observable by enemy).
(6) Airplane (by pick-up and dropped messages, panels).

SECTION VI

MISCELLANEOUS

32. Definitions.—The terms used in these regulations are defined in Basic Field Manual, Volume IV, Signal Communication.

33. Army Regulations and United States Statutes of special applicability.—In addition to AR 105–40, and AR 330–5, the following quoted extracts from United States Statutes contain provisions of special applicability to the subject of these regulations.

Extracts from "The Code of the Laws of the United States of America, in force January 3, 1935"

Title 50, Section 31. Unlawfully obtaining or permitting to be obtained information affecting national defense.—(a) Whoever, for the purpose of obtaining information respecting the national defense with intent or reason to believe that the information to be obtained is to be used to the injury of the United States, or to the advantage of any foreign nation, goes upon, enters, flies over, or otherwise obtains information concerning any vessel, aircraft, work of defense, navy yard, naval station, submarine base, coaling station, fort, battery, torpedo station, dockyard, canal, railroad, arsenal, camp, factory, mine, telegraph, telephone, wireless, or signal station, building, office, or other place connected with the national defense, owned or constructed, or in progress of construction by the United States or under the control of the United States, or of any of its officers or agents, or within the exclusive jurisdiction of the United States, or any place in which any vessel, aircraft, arms, munitions, or other materials or instruments for use in time of war are being made, prepared, repaired, or stored, under any contract or agreement with the United States, or with any person on behalf of the United States, or otherwise on behalf of the United States, or any prohibited place within the meaning of section 36 of this title; or (b) whoever for the purpose aforesaid, and with like intent or reason to believe, copies, takes, makes, or obtains, or attempts, or induces or aids another to copy, take, make, or obtain, any sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, document, writing, or note of anything connected with the national defense; or (c) whoever, for the purpose aforesaid, receives or obtains or agrees or attempts or induces or aids another to receive or obtain from any person, or from any source whatever, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note, of anything connected with the national defense, knowing or having reason to believe, at the time he receives or obtains, or agrees or attempts or induces or aids another to receive or obtain it, that it has been or will be obtained, taken, made, or disposed of by any person contrary to the provisions of this title; or (d) whoever, lawfully or unlawfully having possession of, access to, control over, or being intrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, willfully communicates or transmits or attempts to communicate or transmit the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or (e) whoever, being intrusted with or having lawful possession or control of any document, writing,

code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, or information, relating to the national defense, through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, shall be punished by a fine of not more than $10,000, or by imprisonment for not more than two years, or both. *Act June 15, 1917 (40 Stat. 217; sec. 2181, M. L., 1929).*

Title 50, Section 32. Unlawfully disclosing information affecting national defense.—Whoever, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to, or aids or induces another to, communicate, deliver, or transmit, to any foreign government, or to any faction or party or military or naval force within a foreign country, whether recognized or unrecognized by the United States, or to any representative, officer, agent, employee, subject, or citizen thereof, either directly or indirectly, any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense, shall be punished by imprisonment for not more than twenty years: *Provided*, That whoever shall violate the provisions of subsection (a) of this section in time of war shall be punished by death or by imprisonment for not more than thirty years; and (b) whoever, in time of war, with intent that the same shall be communicated to the enemy, shall collect, record, publish, or communicate, or attempt to elicit any information with respect to the movement, numbers, description, condition, or disposition of any of the armed forces, ships, aircraft, or war materials of the United States, or with respect to the plans or conduct, or supposed plans or conduct of any naval or military operations, or with respect to any works or measures undertaken for or connected with, or intended for the fortification or defense of any place, or any other information relating to the public defense, which might be useful to the enemy, shall be punished by death or by imprisonment for not more than thirty years. *Act June 15, 1917 (40 Stat. 218; sec. 2182, M. L., 1929).*

Title 22, Section 135. Protection of diplomatic codes.—Whoever, by virtue of his employment by the United States, shall obtain from another or shall have custody of or access to, or shall have had custody of or access to, any official diplomatic code or any matter prepared in any such code, or which purports to have been prepared in any such code, and shall willfully, without authorization or competent authority, publish or furnish to another any such code or matter, or any matter which was obtained while in the process of transmission between any foreign government and its diplomatic mission in the United States, shall be fined not more than $10,000 or imprisoned not more than ten years, or both. *Act June 10, 1933 (48 Stat. 122).*

Title 47, Section 605. Unauthorized publication or use of communications.—No person receiving or assisting in receiving, or transmitting, or assisting in transmitting, any interstate or foreign communication by wire or radio shall divulge or publish the existence, contents, substance, purport, effect, or meaning thereof, except through authorized channels of transmission or reception, to any person other than the addressee, his agent, or attorney, or to a person employed or authorized to forward such communication to its destination, or to proper accounting or distributing officers of the various communicating centers over which the communication may be passed, or to the master of a ship under whom he is serving, or in response to a subpena issued by a court of competent jurisdiction, or on demand of other lawful authority; and no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person; and no person not being entitled thereto shall receive or assist in receiving any interstate or foreign communication by wire or radio and use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto; and no person having received such intercepted communication or having become acquainted with the contents, substance, purport, effect, or meaning of the same or any part thereof, knowing that such information was so obtained, shall divulge or publish the existence, contents, sub-

stance, purport, effect, or meaning of the same or any part thereof, or use the same or any information therein contained for his own benefit or for the benefit of another not entitled thereto: *Provided*, That this section shall not apply to the receiving, divulging, publishing, or utilizing the contents of any radio communication broadcast, or transmitted by amateurs or others for the use of the general public, or relating to ships in distress. *Act June 19, 1934 (48 Stat. 1103)*.

Title 47, Section 501. General penalty.—Any person who willfully and knowingly does or causes or suffers to be done any act, matter, or thing, in this chapter prohibited or declared to be unlawful, or who willfully and knowingly omits or fails to do any act, matter, or thing in this chapter required to be done, or willfully and knowingly causes or suffers such omission or failure, shall, upon conviction thereof, be punished for such offense, for which no penalty (other than a forfeiture) is provided herein, by a fine of not more than $10,000 or by imprisonment for a term of not more than two years, or both. *Act June 19, 1934 (48 Stat. 1100)*.

[A. G. 311.5 (3–16–37).]

BY ORDER OF THE SECRETARY OF WAR:

MALIN CRAIG,
Chief of Staff.

OFFICIAL:
E. T. CONLEY,
Major General,
The Adjutant General.

U. S. GOVERNMENT PRINTING OFFICE: 1937

For sale by the Superintendent of Documents, Washington, D. C. - - - - Price 5 cents